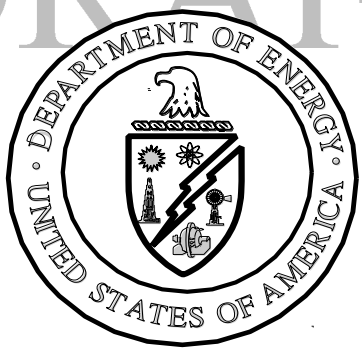
Manual of Protection Requirements

for the

Department of Energy

Classified Information Systems Security Program

DRAFT



11/1/96

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Safeguards and Security

November 1, 1996

DRAFT

(Page Intentionally Blank)

11/1/96

Manual of Protection Requirements for the Department of Energy Classified Information Systems Security Program

DRAFT

1. Purpose. This manual provides requirements and implementation instructions for the graded protection of all classified, and special categories of unclassified information under the security cognizance of NN, automated information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, the Department of Energy (DOE). The requirements are based upon applicable Federal statutes, regulations, National Security directives, Executive Orders, procedures in Office of Management and Budget Circulars and Bulletins, and Federal standards.

2. Applicability. This Manual applies to Departmental Elements responsible for management and operation of the Classified Information Systems Security Program, to ensure the protection of classified information and special categories of unclassified information under the security cognizance of NN, and automated information systems processing this data.

   a. Application to Contracts. The provisions of this Manual are to be applied to covered contractors and they will apply to the extent implemented under a contract or other agreement.

   b. Exclusions. Departmental facilities and activities subject to regulation by the Nuclear Regulatory Commission are exempt from the requirements of this Manual.

11/1/96

3. Summary. All automated information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, DOE requires some level of protection. The loss or compromise of information entrusted to the Department or its contractors may affect the nation's economic competitive position, the environment, the national security, Departmental missions, or the citizens of the United States. The risk management approach defined in this manual for DOE organizations and DOE contractors provides for the graded, cost-effective protection of classified automated information and special categories of unclassified automated information under the security cognizance of NN. Site specific implementations of this manual will be documented by the Classified Site Information Security Plan (SISP). The SISP is an agreement to be executed between each site and the cognizant Headquarters, Operations, or Field Element organization, hereafter referred to as the DOE Office.

4. Definitions. See Attachment 1.

5. Contact. Questions concerning this manual should be directed to Technical and Operations Security of the Policy, Standards, and Analysis Division, Office of

Safeguards and Security, at 301-903-2528.

6. Cancellations. The Manual DOE M 5639.6A-1 is canceled. Cancellation of a Manual does not, by itself, modify or otherwise affect any contractual obligation to comply with such a Manual. Canceled Manuals which are incorporated by reference in a contract shall remain in effect until the contract is modified to delete the reference to the requirements in the canceled Manuals.

DRAFT

11/1/96

Table of Contents

DRAFT 11/1/96

CHAPTER IV

CERTIFICATION AND ACCREDITATION

DRAFT
11/4/96

CHAPTER V

SITE CLASSIFIED INFORMATION SYSTEMS SECURITY PLAN

DRAFT
11/1/96

DRAFT
11/1/96

CHAPTER XI

PROTECTION REQUIREMENTS

DRAFT 11/1/96

ATTACHMENT 1

DRAFT

11/1/96

CHAPTER I

CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM OVERVIEW

1. Introduction. The Department of Energy (DOE) Classified Information Systems Security Program provides for the protection of classified information and special categories of unclassified information under the security cognizance of NN on DOE and DOE contractor information systems[1]. This program consists of four main elements: Management Structure, Risk Management, Requirements, and Infrastructure Support.

2. Management Structure. Management of the Classified Information Systems Security Program is performed through a multi-tiered structure. DOE Office positions include a Department Classified Information Systems Security Program Manager (ISPM) , the Designated Approving Authority (DAA), and the Classified Information Systems Security Operations Manager (ISOM). Positions include the Classified Information Systems Security Site Manager (ISSM) and the Classified Information Systems Security Officer (ISSO). Details of the management structure and responsibilities are described in Chapter II.

3. Risk Management. Risk management is a process that considers the prevailing DOE threat analysis, the effect of countermeasures applied to the processing environment, the remaining vulnerability of the processing environment (residual risk) and the protection requirements and value of the information being processed. Countermeasures are increased until the risk is reduced to an acceptable level or until the cost of reducing the risk becomes prohibitive. Management must then determine if the remaining risk is acceptable or if the automation requirements are sufficient to justify additional costs. Details of the Risk Management Process are in Chapter III.

4. Requirements. The Department's classified information systems security process and the baseline requirement for achieving adequate protection based on level of concern for the confidentiality, integrity and availability of information are detailed in Chapters VII-XI. Additional requirements for interconnected systems (networks) are detailed in Chapter VI.

5. Infrastructure Support. Infrastructure support is provided by the ISPM and includes dissemination of information systems protection information, issuing awareness alerts, conducting workshops, sponsoring training conference(s), providing education for all ISOMs and ISSMs, coordinating an advice and assistance capability, and coordinating an

DRAFT 11/1/96

---

[1]In this manual, the term "system" is used in its general meaning as "Information System or Network". The term is meant to be used so that the distinction between traditional systems and networks is irrelevant to the selection of protection requirements. Special categories of unclassified information under the security cognizance of NN are defined in Attachment 1, page Attachment 1-5.

incident response capability.

a. Education, Awareness, and Training. The DOE Information Systems Security Program requires and depends on knowledgeable personnel. The education, awareness, and training activities shall include:

(1) Education. The ISPM is responsible for ensuring that education in DOE's Information Systems Security policies and practices is available to the ISOMs and ISSMs. The scheduling of these educational activities shall allow all ISOMs and ISSMs to participate within one year of their appointment.

DRAFT

(2) Information Exchange. A capability shall be maintained to facilitate the electronic exchange of Information Systems Security information, such as awareness alerts on sniffer attacks, viruses, etc.

(3) Workshops. The ISPM shall periodically present Information Systems Security workshops.

(4) Information Systems Security Program Conference. The ISPM shall periodically sponsor an information systems security program training conference.

11/1/96

(5) Training. Personnel shall be trained on the information system's prescribed security restrictions and safeguards before they are initially allowed to access a system. This initial training includes the following: threats, vulnerabilities, and risks associated with the information system; information and storage media handling, accessibility, and storage considerations; system data and access controls; and responsibilities associated with the system security. As a follow-up to this initial training, all individuals who access these systems are required to participate in an ongoing security education, training, and awareness program. Such a program shall assure that the individuals accessing the information systems are aware of proper operational and security-related procedures and risks. This training and awareness program includes, but is not limited to, various combinations of: classes (both self-paced and formal), security education bulletins, training films, computer-aided instruction, security briefings, and related educational aids.

b. Advice and Assistance. The ISPM shall support, maintain and coordinate an Advice and Assistance capability for use by any ISOM or ISSM within DOE. The services provided by this capability shall include:

(1) Advice and Assistance Reviews. Reviews of information systems protection as requested by the site, such as reviews of network designs or

protection profiles of networks or systems.

(2) Independent Validation and Verification. Design, certification, and performance test reviews of networks or systems processing classified information with a Protection Level of 5 or 6.

c. Incident Response Capability. The ISPM shall maintain and coordinate an incident response capability to provide timely assistance and system vulnerability information to DOE sites.

d. Technology Development. The ISPM shall provide guidance for a program of technology development to support the DOE Classified Information Systems Security Program. The ISPM shall periodically brief DAAs, ISOMs, and ISSMs on activities and results of the program.

DRAFT

6. Site Information Systems Security Plan (SISP). An agreement between the processing site and the responsible DOE Office that reflects the methodology that the site will employ to meet the protection requirements of the data. Details of the SISP are in Chapter V. The SISP must be approved and implemented before the accreditation cycle is implemented for a system under this new manual. The SISP will be reviewed on the same basis as the Security Plans for the site.

11/1/96

DRAFT

(Page Intentially Left Blank)

11/1/96

CHAPTER II

MANAGEMENT STRUCTURE AND RESPONSIBILITIES

1. Management Structure. Management of the Classified Information Systems Security Program is performed through a multi-tiered structure. The structure includes an ISPM, DAA(s) and ISOM(s) in the DOE Office, and ISSMs and ISSOs in the sites. The following describes the roles of the individuals involved in the decision-making activities in the Program.

DRAFT

a. DOE Classified Information Systems Security Program Manager (ISPM). The Director of the Office of Safeguards and Security (NN-51) shall appoint a DOE employee knowledgeable in IS security to serve as the Program Manager for Classified Information Systems Security. The ISPM shall ensure the implementation of the Classified Information Systems Security Program within the DOE. The ISPM is responsible for the management of the DOE infrastructure that supports the Program. This infrastructure includes an Education, Awareness, and Training Program; an Advice and Assistance Program; an Incident Response Capability; and a technology development effort to provide tools and services to DOE's information systems security practitioners.

11/1/96

b. Designated Approving Authority (DAA). The Manager/Director of each DOE Office shall appoint a DOE employee knowledgeable in IS security to serve as the Designated Approving Authority (DAA) who is responsible for accepting the risk for the loss of confidentiality, availability, and/or integrity of all information systems under the cognizance of the DOE Office and accredits (or reaccredits) each system. The DAA shall ensure the implementation of the Classified Information Systems Security Program within the DOE Office and its cognizant contractors. The DAA shall ensure that all information systems under his/her cognizance provide adequate protection to the information that is processed, created, collected, transmitted or stored on these systems. Some DAA authority may be delegated to other DOE employees.

c. Classified Information Systems Security Operations Manager (ISOM). The Manager/Director of each DOE Office shall appoint one or more individuals knowledgeable in IS security to serve as ISOM(s) to provide technical support to the DAA in the implementation of the Program for information systems under the cognizance of the DOE Office. The ISOM(s) shall oversee the implementation of this Manual for sites under the jurisdiction of the DOE Office, represent DOE in the development of SISPs for each site reporting to the DOE Office, communicate all incident reports received from sites to the ISPM, ensure the SISP provides protection at least equivalent to the requirements of this Manual , and regularly review the program at each site under the jurisdiction of the DOE Office. The same person may be appointed as both the DAA and ISOM.

d. Classified Information Systems Security Site Manager (ISSM). The Manager of each site shall appoint an ISSM to implement the Classified Information Systems Security Program for information systems at the site. The ISSM shall ensure the development of the SISP and the management of the Program for the site.

e. Classified Information Systems Security Officer (ISSO). The ISSO is responsible for ensuring that protection features are installed and operational in an information system.

2. Responsibilities.

a. Classified Information Systems Security Program Manager (ISPM) shall:

(1) Develop and recommend DOE policies, standards, procedures, and guidelines for the protection of information systems that collect, create, process, transfer, store, or provide access to classified information or special categories of unclassified information under the security cognizance of NN.

(2) Maintain a continuing review of this manual to assure that current technology is being applied to the protection of information systems that create, process, store, transfer, or provide access to classified information or special categories of unclassified information under the security cognizance of NN and to eliminate those practices that are no longer needed or effective.

(3) Approve secure remote diagnostic and maintenance facilities proposed for use with information systems that process classified information.

(4) Perform an annual review and update, as needed, of the Annual DOE Classified Information Systems Security Program Risk Assessment and the DOE Statement of Threat to classified information systems.

(5) Designate the DAA for information systems that involve multiple DAA(s) and accredit systems operating at a protection level of 5 or 6.

(6) Establish a Classified Information Systems Security Program infrastructure that includes at a minimum, education, awareness and training; advice and assistance; technology development; and an incident response capability.

(7) Represent the DOE before Federal, private, and public organizations concerned with the protection of classified information systems.

DRAFT 11/1/96

(8) Report changes in ISOM and DAA appointments to all DAA(s).

(9) Coordinate:

(a) With the Unclassified Computer Security Program Manager.

(b) With the Office of Intelligence on the protection of Sensitive Compartmented Information.

(c) The implementation of the Classified Information Systems Security Program with the Classified Material Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Distribution Systems, TEMPEST, Materials Control and Accountability, and other programs, as appropriate.

DRAFT

(d) The development, publishing, and distribution of guidelines for the protection of classified information systems.

(f) The development, presentation, and maintenance of classified information systems security education programs for ISOM(s) and ISSM(s).

(10) Provide:

11/1/96

(a) Overall guidance and direction for field assistance and technology development for classified information systems security.

(b) Guidance and direction for education, awareness, and training activities for the Classified Information Systems Security Program.

(c) Guidance for the DOE Computer Incident Advisory Capability.

(d) Collection and dissemination of information relevant to the Classified Information Systems Security Program.

(e) Monitoring of the Classified Information Systems Security Program findings and deficiencies resulting from surveys, inspections, and reviews.

(f) A timely review of the protection documentation for information systems located in Sensitive Compartmented Information Facilities that process, store, transfer, or provide access to intelligence information and the certification of the information system received from cognizant ISOM(s) and comments, to the Office of Intelligence.

b. DOE Office Manager. The Manager of each DOE Office that uses information systems shall:

(1) Appoint, in writing, a DOE employee to serve as the DAA for information systems under the cognizance of the DOE Office. Notify the ISPM of this appointment. The same person may be appointed as both the DAA and ISOM.

(2) Appoint, in writing, one or more DOE employee(s) knowledgeable in information systems security as the ISOM(s) for classified information systems under the cognizance of the DOE Office. Notify the ISPM of this appointment. The same person may be appointed as both the DAA and ISOM.

DRAFT

(3) Ensure:

(a) The implementation of this manual for information systems under their management and control, including those of contractors under the cognizance of the DOE Office.

(b) That the ISOM(s) and all ISSM(s) at sites under their jurisdiction receive ISPM-sponsored training in the DOE Classified Information Systems Security Program within 1 year of appointment.

11/1/96

c. Designated Approving Authority. The DAA shall be responsible for evaluating the protection measures in a system as described in the Systems Security Plan (SSP), the results of any certification tests, the certification of the system, and any residual risks of operating the system. The DAA shall:

(1) Have written authorization to accept the residual risk and responsibility for all classified information systems under his/her jurisdiction. The authorization shall include provisional accreditation, withdrawal of accreditation, and suspension of operations for all classified information systems under his/her jurisdiction.

(2) Approve SISPs for each site under the cognizance of the DOE Office,

(3) Serve as accrediting authority for each DOE and covered contractor classified information system.

(4) Ensure each classified information system under his/her jurisdiction is accredited or reaccredited at least every 3 years (except for information systems processing Sensitive Compartmented Information) and that the accreditation or reaccreditation is documented.

(5) Ensure DAA authorities are delegated to DOE employees who are knowledgeable individuals.

(6) Report any changes in ISOM or ISSM appointments to the ISPM.

d. Classified Information Systems Security Operations Manager(s) (ISOM) shall:

(1) Represent the DOE Office in the negotiation of SISPs for each site reporting to the DOE Office.

(2) Communicate incident reports received from sites to the ISPM.

(3) Review SISPs and provide recommendations to the DAA.

(4) Ensure the regular review of the Classified Information Systems Security Program at each site under the jurisdiction of the DOE Office.

(5) Evaluate information systems for accreditation when requested by the DAA.

(6) Monitor the responses to findings and other deficiencies identified in surveys, inspections, and reviews of each site Classified Information Systems Security Program to ensure that any necessary corrective or compensatory actions have been completed.

(7) Coordinate:

(a) The Classified Information Systems Security Program with the unclassified information systems security program.

(b) The implementation of the Classified Information Systems Security Program with the Classified Material Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Distribution Systems, TEMPEST, Materials Control and Accountability, and other programs, as appropriate.

e. Site Manager(s) where information systems are operated shall ensure:

(1) The implementation of a Classified Information Systems Security Program in accordance with the approved SISP.

(2) That managers and supervisors are aware of, and fulfill, their responsibilities for the protection of classified information.

(3) The identification and funding of the independent validation and

DRAFT 11/1/96

verification of classified information systems with a Protection Level of 5 or 6.

(4) The appointment, in writing, of an ISSM who is responsible for the implementation of the site Classified Information Systems Security Program as defined in the SISP. A seperate ISSM may be appointed for information systems in a Sensitive Compartmented Information Facility if the site determines that another ISSM is needed.

(5) That the ISSM(s) under his/her jurisdiction participate in ISPM-sponsored information systems security education within 1 year of appointment.

(6) Report any changes in ISSM appointments to the cognizant DAA(s).

DRAFT

f. Classified Information Systems Security Site Manager(s) (ISSM) shall:

(1) Ensure the development of the SISP for the site.

(2) Act as the site point of contact for all classified information systems security activities, including inspections, tests, and reviews.

(3) Ensure the development, documentation, and presentation of information systems security education, awareness and training activities for site management, information security personnel, data owners, and users.

11/1/96

(4) Ensure the development, documentation, and presentation of information systems security training for escorts for information systems.

(5) Establish, document, implement, and monitor the Classified Information Systems Security Program for the site and assure site compliance with DOE policies, standards, and procedures for information systems.

(6) Ensure the development of procedures for use in the site's classified information systems security program.

(7) Identify and document unique threats for information systems at the site.

(8) Ensure that the site's Classified Information Systems Security Program is coordinated with the Site Safeguards and Security Plan or the Site Security Plan.

(9) Coordinate:

(a) Implementation of the site Classified Information Systems Security Program with the Classified Material Protection and Control,

Personnel Security, Physical Security, Communications Security, Protected Distribution Systems, TEMPEST, Materials Control and Accountability, and other site programs, as appropriate.

(b) Development of a site self-assessment program for the Classified Information Systems Security Program.

(c) Performance of a self-assessment of the site Classified Information Systems Security Program, between surveys.

(10) Ensure the development of site procedures to govern marking, handling, controlling, removing, transporting, sanitizing, reuse, and destruction of media and equipment containing classified information.

DRAFT

g. Classified Information Systems Security Officer(s) ISSO shall:

(1) Ensure the implementation of security measures for each classified information system for which he/she is responsible.

(2) Prepare, maintain, and implement a Classified Systems Security Plan (SSP) that accurately reflects the installation and security provisions for each classified AIS for which he/she is responsible.

11/1/96

(3) Identify and document any unique threats for the classified information systems for which he/she is the ISSO and forward to the ISSM.

(4) Perform a risk assessment to determine if additional countermeasures beyond those identified in this Manual are required, if so directed by the DAA and/or an identified unique local threat exists.

(5) Develop and implement a certification test plan for each classified information system operating at a Protection Level of 4, 5, or 6 for which he/she is the ISSO.

(6) Advise the ISSM, in writing, that the Classified Information Systems Security Program has been implemented as described in the SSP and that the specified security controls are in place and properly implemented.

(7) Maintain the record copy of the Classified Systems Security Plan and related documentation for each classified Information Systems for which he/she is the ISSO.

(8) Ensure:

(a) The development, documentation, and testing, if required, of a

continuity of operations plan based on guidance from the responsible management official.

(b) That each classified information system for which he/she is responsible is covered by the site Configuration Management Program.

(c) That the proper sensitivity level of the information is determined prior to use on the classified information system and that the proper security measures are implemented to protect this information.

DRAFT

(d) That unauthorized personnel are not granted use of, or access to, a classified information system.

(e) The implementation of formal access controls for each classified information system, except personal computers and standalone workstations.

(9) Document any special security requirement identified by the data owners and the protection measures implemented to fulfill these requirements for the information contained in the classified information system.

11/1/96

(10) Implement site procedures:

(a) To govern marking, handling, controlling, removing, transporting, sanitizing, reuse, and destruction of media and equipment containing classified information.

(b) To ensure that vendor-supplied authentication (password, account names) features or security-relevant features are properly implemented.

(c) For the reporting of classified information systems security incidents.

(d) Requiring that each classified information system user sign an acknowledgement of responsibility (Code of Conduct) for the security of classified information systems and classified information.

(e) For the detection of malicious code, viruses and intruders (hackers).

(11) Identify classified Information Systems Security training (including

system-specific training) needs to ensure that system users are properly trained and recommend personnel to attend training programs.

(12) Conduct classified information systems ongoing security reviews and testing to periodically verify that security features and operating controls are functional and effective.

(13) Evaluate proposed changes or additions to the classified information systems and advise the ISSM of their security relevance.

DRAFT

11/1/96

DRAFT

(Page Intentially Left Blank)

11/1/96

CHAPTER III

RISK MANAGEMENT PROCESS

1. Introduction. The cornerstone of DOE's Classified Information Systems Security Program is the risk management process which determines the protection requirements for DOE's information. Risk management balances the data owner's perceived value of the information and the data owner's assessment of the consequences of loss of confidentiality, integrity and availability against the costs of protective countermeasures and day to day operations. DOE's risk management process includes the following interrelated phases:

DRAFT

- Threat analysis;
- Countermeasure analysis where the generic threats, technologies and architectures are evaluated and integrated into DOE policies, guidelines, and standards;
- Data owner declaration of the consequences of loss of confidentiality, integrity and availability;
- Site program implementation where the unique concerns of the site (i.e., threats, protective technologies, procedures, etc.) are evaluated and integrated with site operations;
- System implementation where the impact of information loss; system vulnerabilities; data owner protection requirements; cost of protective measures; and mission requirements are identified, evaluated, and integrated;

11/1/96

- System operation where the remaining risk (residual risk) is accepted and oversight is initiated to ensure that the level of residual risk is managed throughout the information system's life cycle. Information system incident reporting contributes to risk management by providing timely notification of incidents that may affect the protection features in other information systems; and
- Oversight activities which support and improve the risk management approach through reviews of the information systems security program implementation in the DOE Offices and sites.

2. Threat Analysis. The analysis of information threats identified by National and DOE organizations provides the basis for protecting DOE's classified information and special categories of unclassified information under the security cognizance of NN. The ISPM shall annually review the Nation's information threat posture. The results of this review shall be used to develop or update the DOE Statement of Threat.

3. Departmental Risk Analysis. This process begins with an analysis of information architectures and technologies to determine how information with different sensitivities can be protected on an information system. A risk assessment is then performed using this analysis and the DOE Statement of Threat. The results of this risk assessment are

used as the basis to develop the protection countermeasures for DOE's information.

a. DOE Risk Assessment. The ISPM shall maintain a constant awareness of technology, technology trends, information architectures, and information standards as they relate to protecting information. This information, and the DOE Statement of Threat, shall be used by the ISPM to perform the DOE Risk Assessment.

b. Changes to Policy and Guidelines. If either the DOE Statement of Threat or the DOE Risk Assessment are changed, the ISPM shall conduct an analysis to identify and recommend changes to DOE Policy in this Manual.

DRAFT

4. Data Owner Responsibilities. The owner of each piece of information collected, created, processed, transmitted, or stored on an automated information system is expected to . declare the level of sensitivity or classification of information on the automated system. If no data owner declaration is available, the Protection Profiles defined in the SISP shall document the minimum protection requirements applied to information by the site.

5. Site Program Implementation. The SISP enables the site to customize the DOE Classified Information Systems Security Program to the site's operational needs. The SISP integrates data owner information protection requirements, site unique threats, site unique protection technologies, cost of protective measures, and mission impact with the DOE Classified Information Systems Security Program. The following decisions and activities are fundamental to, and shall be included in, any site plan for classified information systems protection.

11/1/96

a. Site Risk Assessment. The DOE Risk Assessment and any site specific threats shall be incorporated into a site risk assessment. The site risk assessment shall consider any protection technologies unique to the site, the cost of protection measures, the information protection requirements, and the impact of protection measures on the information system mission. The results of the site risk assessment shall be used to define the classified information systems protection profiles to be applied to information systems at the site. The results of the risk assessment shall be documented.

b. Levels of Concern, Protection Level, and Protection Profiles. Describing information systems protection with levels of concern, protection levels, and protection profiles provides consistency of description across the Department.

(1) Protection Profile Documentation. The Levels of Concern, Protection Level, and associated Protection Profiles that are the basis of the site's protection program shall be documented in the SISP.

(2) Protection Profiles. The Protection Profiles defined by a site for information systems processing DOE information shall provide protection at least equivalent

to the Protection Profiles in the Manual.

c. SISP Approvals. The SISP shall be approved by both the Site Manager and the cognizant DOE Office Designated Approving Authority. A SISP for a DOE Office shall be approved by the DOE Office Manager.

6. New or Modified System Implementation. The system implementation process begins with identifying the level of concern and protection level of the information to be processed. The protection profile is determined based on the levels of concern and protection level. The protection profile requirements are then integrated into the information systems design, implementation, and operation.

7. System Operation. The final phase of the risk management process is the acceptance of risk through certification and accreditation, and the protection of information during day-to-day operations.

8. DOE Incident Reporting. The ISOM shall ensure that incidents affecting DOE or national interests are reported (via telephone or other electronic means) to the ISPM. The report shall include at least the location of the incident, possible effect on DOE or national interests, a description of the incident, and a description of the actions taken to protect information after the incident was discovered. All individual(s) collecting information about or reporting an incident shall ensure that any sensitive or classified information involved in the incident or report is properly protected.

a. The incident reporting requirements are:

(1) Affects Site Interests. If the incident affects only site interests, the site shall collect and maintain information about incidents, such as location, description, resources needed to respond to the incident, and actions taken to protect information after the incident was discovered. This information shall be available on request from the DAA. A quarterly summary report shall be submitted to the ISPM.

(2) Affects DOE or National Interests. If the incident affects DOE or national interests, the incident shall be reported to the ISOM immediately after detection. The ISOM shall report the incident to the ISPM within one hour after receiving the site report.

b. The ISPM will issue instructions relating to information to be reported.

9. Oversight. Periodic evaluations of the site Classified Information Systems Security Program are required to ensure that the program continues to function in accordance with the SISP.

a. ISOM Program Reviews. The ISOM shall ensure that periodic reviews of the

DRAFT 11/1/96

site's Classified Information Systems Security Program are performed to ensure that it continues to implement the site's SISP.

b. ISSM Self Assessments. The ISSM shall ensure that periodic assessments of the site's program, including the content of the SISP, are performed. The frequency of the reviews shall be documented in the SISP. Upon completion of each review, the ISSM shall ensure the preparation and implementation of an action plan for all identified findings or vulnerabilities as directed by DOE Order 470.1, Chapter IX, Paragraph 10. a. A record of each review and the subsequent action plan shall be maintained and available for future inspections.

DRAFT

11/1/96

CHAPTER IV

CERTIFICATION AND ACCREDITATION

1. Overview. The certification and accreditation process begins after the protection measures have been implemented on a system and any required information systems protection documentation has been approved. The certification process validates that a protection profile has been selected, that the protection profile has been implemented on the system, and that the protection measures are functioning properly. This process culminates in an accreditation for the system to operate.

2. Certification Process. The certification process subjects the system to appropriate verification that it has been implemented in accordance with the selected protection profile and validates that each required protection measure has been implemented.

DRAFT

   a. Independent Validation and Verification. For information systems intended to operate in protection levels 5 and 6, an Independent Validation and Verification (IV&V) review shall support the certification process.

   b. Sensitive Compartmented Information. For information systems that process sensitive compartmented information and are located in a Sensitive Compartmented Information Facility, the cognizant ISSM, ISOM and ISPM shall review the information system protection documentation and the certification of the information system and direct it, with their comments, to the Office of Intelligence, Office of Nonproliferation and National Security.

11/1/96

3. Accreditation. All systems shall be reviewed and accredited to operate by the DAA.

   a. Provisional Accreditation. The DAA may grant provisional accreditation (temporary authority) to operate an information system because of incomplete documentation , or to permit a major conversion of the information system. This provisional accreditation may be granted for up to 180 days. DAA-approved protection measures shall be in place and functioning during the period of provisional accreditation.

   b. Reaccreditation. Following the intent of OMB Circular A-130, "Management of Federal Information Resources," each information system shall be reaccredited every 3 years at a minimum. Information system accreditation shall be reviewed immediately if there are modifications to the information system that impact its protection, if the protection aspects of its environment change, or if the applicable protection requirements change.

   c. Withdrawal of Accreditation. The DAA shall evaluate the risks and consider withdrawal of accreditation if the protection measures and controls approved for the system do not remain effective or whenever changes occur to any of the

following: levels of concern, protection level; technical or nontechnical security safeguards, vulnerabilities, operational environment, operational concept, or interconnections.

d. Certification and Accreditation of Multiple Systems. Where two or more similar information systems are to be operated in equivalent operational environments (i.e., the Levels of Concern and Protection level are the same and the physical security requirements are similar), a Master Systems Security Plan (SSP) may be written and approved by the DAA , to cover all such information systems. The information systems covered by a Master SSP may range from personal computers up to and including multiuser information systems and local area networks that meet the criteria for a master plan approach.

DRAFT

(1) Master Systems Security Plan. The Master SSP for these information systems shall specify the information required for each certification for an information system to be accredited under the plan.

(2) Information Systems Documentation. For information systems covered by Master SSPs, the ISSM shall ensure that each information system is documented with 1) the information system identification, 2) the information system location, 3) the Master SSP covering the information system, and 4) a statement certifying that the information system implements the requirements in the Master SSP signed by the ISSO.

11/1/96

(3) Information Systems Accreditation. The DAA shall accredit the first information system under the Master SSP. All other individual information systems to be operated under the Master SSP shall be certified by the ISSM as meeting the conditions of the approved Master SSP. This certification, in effect, accredits the individual information systems to operate under the Master SSP. A copy of each certification report shall be retained with the approved copy of the Master SSP.

(4) Recertification of Information Systems. All information systems certified under a Master SSP remain certified until the Master SSP is changed or 3 years have elapsed since the information system was certified . If the level of concern or protection level described in the Master SSP change, all information systems certified under the Master SSP shall be re-certified.

4. Designated Approving Authority. :

a. Systems at Protection Levels 5 and 6. The ISPM shall be the DAA for systems at protection levels 5 and 6.

b. Delegation of Approval Authority. The DAA may delegate accreditation authority. Rules for this delegation are

(1) All delegations shall be in writing and for a specified time period not to exceed three years.

(2) The DAA (or his/her delegate) and the person certifying the system shall not be the same person.

(3) The delegate cannot redelegate the accrediting authority.

(4) The delegate must be a federal employee.

c. Systems under Multiple Approving Authorities. For systems that involve multiple DAAs, the ISPM shall serve as or select the approving authority. Each site involved in the system shall identify, in writing, the security officials to be responsible for implementing information system protection on the system components at the site.

d. Director of Naval Reactors Program. For information systems networks that are solely under the jurisdiction of the Director of Naval Reactors Program and whose external components extend into the jurisdiction of different Naval Reactor Offices, the Director of Naval Reactors Program shall designate one of the Naval Reactor Office senior managers to be the DAA. Notification of the accreditation of any information system with a protection level of 4, 5, or 6 shall be furnished to the ISPM.

5. Alternative Protection Means and Deviations. Where it is impossible or impracticable to implement the protection requirements and countermeasures described in this manual in the classified information system, alternative protection means and deviations (variances, waivers, or exceptions) shall be approved under the procedures described in DOE 470.1.

DRAFT 11/1/96

DRAFT

(Page Intentially Left Blank)

11/1/96

CHAPTER V

SITE CLASSIFIED INFORMATION SYSTEMS SECURITY PLAN

1. Introduction. The Site Classified Information Systems Security Plan (SISP) is an agreement, between the DOE Office and the site, for the protection of information. The SISP describes the Site Classified Information Systems Security Program and the implementation details for information protection measures applied to the site's information systems. The SISP shall be the basis for all decisions on, and evaluations of, information systems security at the site. If the site's information protection requirements are diverse, the SISP may contain multiple sections covering different parts of the site's information systems security program.

DRAFT

2. Required Contents. A SISP shall address at least the following topics. Additional topics may be added to the SISP if required for site-unique information protection requirements.

   a. Site Classified Information Systems Security Program Description. The SISP shall contain an overview of the Classified Information Systems Security Program at the site. The overview shall describe how the site program applies to site subcontractors.

   b. Risk Assessment. The SISP shall contain or reference the site risk assessment.

   c. Protection Profiles. The SISP shall contain a description of the site processes to:

11/1/96

      - determine any data owner information protection requirements,
      - determine the levels of concern and processing mode,
      - select the protection profile, and
      - integrate the protection requirements into the system design, implementation and operation.

   d. Rules of Use. The SISP shall contain a description of how information system users are informed of, and accept, their responsibilities for protecting information and computing resources, including the protection of information accessed or controlled by the user, and for complying with the operating rules of the information system Code of Conduct. Personnel shall sign the appropriate nondisclosure agreement or privacy-act agreement form(s) for all the information on systems to which they have been granted access. The Code of Conduct will be an attachment to the SISP.

   e. Site-Wide Procedures. The SISP shall identify the procedures, such as interconnection to external information systems, escort responsibilities, incident reporting and response, detecting misuse of computing resources, the management of user identifiers, media management, protection testing, and self-

assessment, to be used in the Site Classified Information Systems Security Program. The SISP shall contain an explanation of how the procedures are reviewed and updated.

f. Education, Awareness, and Training Activities. The SISP shall contain or reference the plan for education, awareness, and training of the site management, information systems security personnel, system users, and data owners.

g. Sensitive Compartmented Information. The SISP shall contain a description of the application of this manual to information systems within a Sensitive Compartmented Information Facility (SCIF) at the site. However, the requirements in this Manual may not fully represent the protection requirements for processing intelligence information. Additional requirements may be established by the intelligence community. The additional requirements are not required to be documented in the SISP.

3. Classified Information Systems Security Program Personnel. The site personnel responsible for management of the site program shall be identified in an appendix to the SISP. This appendix shall be used only to identify the individuals and shall not be included in the SISP review and approval process.

DRAFT
11/1/96

CHAPTER VI

REQUIREMENTS FOR INTERCONNECTED SYSTEMS

1. Interconnected Systems Management. The characteristics and capabilities of classified systems implemented as networks require special security considerations. This chapter imposes additional requirements on a network or expands on the security requirements stated in Chapters X and XI as they apply to a network.

   a. When connecting two or more networks, the DAA(s) shall review the security attributes of each network (even if the networks are accredited at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.

   b. A unified network is a connected collection of systems or networks that are accredited (1) under a single security plan, (2) as a single entity, and (3) by a single DAA. Such a network can be as simple as a small standalone LAN operating at a Protection Level of 1, following a single security policy, accredited as a single entity, and administered by a single ISSO. Conversely, it can be as complex as a collection of hundreds of LANs separated over a wide area but still following a single security policy, accredited as a single entity by a single DAA. The perimeter of each network encompasses all its hardware, software, and attached devices. Its boundary extends to all of its users.

   c. An interconnected network is comprised of two or more separately accredited systems and/or networks. Each separately accredited system or network maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating system or network has its own ISSO. The interconnected network shall have a Security Support Structure (SSS) capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires accreditation as a unit.

   d. Systems that process information at differing classification levels or with differing compartmentation (i.e., at least two kinds of information that require different formal access approvals) can be interconnected if:

      (1) They are interconnected through a Controlled Interface (as defined below) that provides the separation appropriate to the combination of the level(s) and compartment(s) being processed on both systems; or

      (2) If both systems are operating at the same Protection Level, both systems must be accredited to protect the information being transferred; or

DRAFT 11/1/96

(3) Both systems are accredited to process the level(s) and compartment(s) of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.

e. Any classified system connected to another system that does not meet either (2) or (3) above shall utilize a Controlled Interface(s) (CI) that performs the following:

(1) A communication of lower classification level from within the system perimeter shall be reviewed for classification before being released.

(2) A classified communication from within the system perimeter shall have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

DRAFT

(3) Communications from outside the system perimeter shall have an authorized user as the destination (i.e., the CI shall notify the user of the communication and release the communication only on request from the user). If classified information exists in the communication, it shall be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

2. Controlled Interface Functions. The functions of the Controlled Interface (CI) include (1) providing a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts; (2) providing a reliable exchange of security-related information; or (3) filtering information in a data stream based on associated security labels for data content. CIs have several characteristics including:

11/1/96

a. There are NO GENERAL USERS on the CI;

b. There is NO USER CODE running on the CI;

c. The CI provides a protected conduit for the transfer of user data; and

d. Communications from outside the perimeter of the system shall be reviewed for viruses and other malicious code.

3. Controlled Interface Requirements. The CI shall have the following properties:

a. Adjudicated differences. The CI shall be implemented to monitor and enforce the protection requirements of the network and adjudicate the differences in security policies.

b. Routing decisions. The CI shall base its routing decisions on information that is

supplied or alterable only by the SSS.

c. Restrictive protection requirements. The CI shall support the protection requirements of the most restrictive of the attached networks or information systems.

d. User code. The CI shall not run any user code.

e. Fail-secure. The CI shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.

f. Communication Limits. The CI shall ensure that communication policies and connections that are not explicitly permitted are prohibited.

g. The platform on which the CI is operating usually need meet no more than the technical protection requirements for Protection Level 3. In general, such systems have only privileged users; i.e., system administrators and maintainers. The CI may have a large number of clients (i.e., individuals who use the CI's functional capabilities in a severely constrained way). The CI application, itself, will have to provide the more-stringent technical protections appropriate for the system's protection level. Multiple applications do not affect the overall protection provided by the CI if each application (and the resources associated with it) are protected from unauthorized access or circumvention from other applications or users.

DRAFT 11/1/96

4. Assurances for CIs. Each CI shall be tested and evaluated to assure that the CI, as implemented, can provide the separation required for the system's protection level. Specifically, the platform on which the CI runs does not necessarily have to provide the needed separation, alone.

DRAFT

(Page Intentially Left Blank)

11/1/96

CHAPTER VII

PROTECTION PROFILES

1. Introduction. A Protection Profile (PP) describes the protection measures that must be addressed throughout the system lifecycle. A PP contains (1) a description or definition of the system environment addressed by the PP, (2) the confidentiality measures that must be addressed, (3) the integrity measures that must be addressed, and (4) the availability measures that must be addressed. The SISP shall describe the process used to determine the protection profiles for site information systems.

DRAFT

2. Levels of Concern. The Level of Concern reflects the data owner's perceived value of the information and the consequences of the loss of integrity, availability, or confidentiality. If the data owner has not established the level of concern , the data steward, with the assistance of the ISSO, will do so. The SISP shall contain a description of the Levels of Concern and the process for determining the level of concern. The levels of concern are listed in Chapter VIII.

3. Protection level. The Protection Level describes the information system's user community. The SISP shall contain a description of the site Protection Levels and the process for determining the protection level. The protection levels are based on the users' need-to-know, formal access approval(s), and access authorizations (clearances). These protection levels are defined in Chapter IX.

11/1/96

4. Embedded Systems. Some systems cannot be altered without special hardware or software not generally available to users, and are designed and implemented to provide a very limited set of predetermined functions. Certain "embedded" systems fall in this category. If the DAA concurs that such a system is sufficiently incapable of alteration, and that the system provides an adequate level of security, then the system does not have to meet additional security requirements specified for more-general-purpose systems in this manual. DAA, DAA designees, and implementors are cautioned to be sure that such systems, in all operational situations, provide the separation appropriate to the system's protection level.

5. Protection Profiles. Protection Profiles organize protection measures into a set of requirements. The requirements are graded, based on the Levels of Concern and Protection Level, and include any information protection requirements defined by the data owner. The Protection Profile for a specific information system is based on the information the Levels of Concern and the Protection Level. The SISP shall contain a description of the site protection profiles and the process for selecting a protection profile. A protection profile shall contain the following items:

   a. Confidentiality Components. A description of the confidentiality protection

requirements that must be implemented in an information system using the profile. The confidentiality protection requirements shall be graded according to the confidentiality protection levels which incorporate levels of concern.

b. Integrity Components. A description of the integrity protection requirements that must be implemented in an information system using the profile. The integrity protection requirements shall be graded according to the integrity levels of concern.

c. Availability Components. A description of the availability protection requirements that must be implemented in an information system using the profile. The availability protection requirements shall be graded according to the availability levels of concern.

DRAFT

d. Common Requirements. Requirements that are common to all systems are detailed in Chapter X - Baseline Requirements.

e. Graded Requirements. Requirements that are graded by level of concern and confidentiality protection level are detailed in Chapter XI - Protection Requirements. The following tables present in tabular form the requirements detailed in Chapter XI - Protection Requirements. To use these tables, find the column representing the protection level for confidentiality, or find the column representing the level of concern for integrity and availability.

11/1/96

6. Protection Level (PL) Table for Confidentiality.

Requirements (Page)						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Audit Capability (XI-2)	AUD-1	AUD-1	AUD-2	AUD-3	AUD-4	AUD-4
Communications (XI-5)	COM-1	COM-1	COM-1	COM-2	COM-1	COM-1
Configuration Management (XI-7)	CM-1	CM-1	CM-1	CM-2	CM-3	CM-3
Independent Validation and Verification (XI-9)					IVV-1	IVV-1
Resource Access Control (XI-10)		RAC-1	RAC-1	RAC-2	RAC-3	RAC-3
Resource Utilization (XI-11)	RU-1	RU-1	RU-1	RU-2	RU-2	RU-2
Session Controls (XI-12)	SC-1	SC-2	SC-2	SC-3	SC-3	SC-3
Security Documentation (XI-13)	SD-1	SD-1	SD-2	SD-2	SD-3	SD-3
Separation of Functions (XI-16)				SF-1	SF-1	SF-1
System Recovery (XI-16)	SR-1	SR-1	SR-1	SR-1	SR-2	SR-2
Security Support Structure (XI-17)	SSS-1	SSS-1	SSS-1	SSS-2	SSS-3	SSS-3
Security Testing (XI-18)	ST-1	ST-2	ST-2	ST-3	ST-4	ST-4
Trusted Path (XI-20)					TP-1	TP-1

DRAFT
11/1/96

7. Level of Concern Table for Integrity.

Requirements (Page)			
Integrity	Low	Medium	High
Audit Capability (XI-1)	AUD-1	AUD-2	AUD-4
Backup and Restoration of Data (XI-3)	BRD-1	BRD-2	BRD-3
Changes to Data (XI-4)	CD-1	CD-2	CD-3
Communications (XI-5)	COM-1	COM-1	COM-2
Configuration Management (XI-7)	CM-1	CM-2	CM-3
Security Support Structure (XI-17)	SSS-1	SSS-2	SSS-3
Security Testing (XI-18)	ST-1	ST-3	ST-4

8. Level of Concern Table for Availability.

Requirements (Page)			
Availability	Low	Medium	High
Alternative Power Source (XI-1)	APS-1	APS-2	APS-3
Disaster Recovery Planning (XI-8)	DRP-1	DRP-2	DRP-3
Security Support Structure (XI-17)	SSS-1	SSS-2	SSS-3

DRAFT
11/1/96

CHAPTER VIII

LEVELS OF CONCERN

1. Information Sensitivity Matrices. The following tables are designed to assist those involved in system development, implementation, certification, and accreditation in determining the appropriate level of concern for confidentiality, integrity, and availability for a given system processing a given set of information. General guidelines in how to use the Information Sensitivity Matrix would include:

   a. A determination of high, medium, or low shall be made for each of the three attributes: confidentiality, integrity, and availability. It is not necessary for the level of concern to be the same for all attributes of the system.

   b. When a given system has more than one kind of information on it, the level of concern for the system is the highest of the levels of concern for each of the kinds of information.

   c. The information sensitivity matrices were constructed to assist the DAA in considering the sensitivity of the information and in selecting the level of concern for confidentiality, integrity, and availability. The DAA shall use guidance from the data owner(s) in making this decision.

   d. The DAA or the data owner may choose to apply a higher level of concern for any aspect of any information on the system.

2. Confidentiality Level of Concern. In considering confidentiality, the principal question is the necessity for maintaining the classification levels and the types of information (e.g. SRD Sigma 15) on the system in question. The protection level table for confidentiality combines the processing environment with the level of concern for confidentiality to provide a set of graded requirements to protect the confidentiality of the information on the system. **This graded approach to risk provides sufficient and necessary protection for the information on the system without requiring unnecessary protections for systems where the level of concern for confidentiality is low or medium**.

DRAFT
11/1/96

Information Sensitivity Matrix
for
Confidentiality

Level of Concern	Qualifiers
High	All Sensitive Compartmented Information All SAPs/SARs All Information Protecting Intelligence Sources, Methods and Analytical Procedures All SIOP All Crypto SECRET RD (SIGMAs 1,2,14,15) TOP SECRET
Medium	SECRET SECRET RD (All other SIGMAs)
Low	CONFIDENTIAL CONFIDENTIAL RD Special Categories of Unclassified Information Under the Security Cognizance of NN

NOTE: The data owner may specify a level of concern that exceeds what is warranted by the table.

DRAFT
11/1/96

3. Integrity Level of Concern. In considering integrity, the principal question is the necessity for maintaining the integrity of the information **on the system in question**.

Information Sensitivity Matrix
for
Integrity

Level of Concern	Qualifiers
High	Absolute accuracy required for mission accomplishment; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.
Medium	High degree of accuracy required for mission accomplishment, but not absolute; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.
Low	Reasonable degree of accuracy required for mission accomplishment; or loss of integrity will have an adverse effect.

DRAFT

11/1/96

4. Availability Level of Concern. In considering availability, the principal consideration is the need for the information **on the system in question** to be available in a fixed time frame to accomplish a mission.

Information Sensitivity Matrix
for
Availability

Level of Concern	Indicators
High	Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.
Medium	Information must be readily available with minimum tolerance for delay; or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.
Low	Information must be available with flexible tolerance for delay; or loss of availability will have an adverse effect.

NOTE: In this context "High - No tolerance for delay" means no delay; "Medium - minimum tolerance for delay" means a delay of seconds to minutes; and "Low - flexible tolerance for delay" means a delay of days to weeks.

DRAFT
11/1/96

CHAPTER IX

PROTECTION LEVELS

1. Introduction. The protection level is determined by the relationship between two sets of facts: first, the clearance(s), formal access approval(s), and need-to-know of users; and second, the classification, formal access requirements, and sensitivity of the information on the system. It indicates an implicit level of trust that is placed in the system's technical capabilities.

2. Protection Levels. The table at the end of this chapter presents the criteria for determining six protection levels:

DRAFT

a. Systems are operating at Protection Level 1 when **all** users have all required approvals for access to all information on the system. For systems processing classified information, this means that all users have all required clearance(s), formal access approval(s), and the need to know for all information on the system.

b. Systems are operating at Protection Level 2 when **all** users have all required **formal** approval(s) for access to all information on the system, but at least one user lacks administrative approval(s) for some of the information on the system. For systems processing classified information, this means that all users have all required clearance(s) and all required formal access approval(s), but at least one user lacks the need to know for some of the information on the system and **no information on the system has a classification level higher than Confidential** (i.e., the level of concern for confidentiality is low).

11/1/96

c. Systems are operating at Protection Level 3 when **all** users have all required **formal** approval(s) for access to all information on the system, but at least one user lacks administrative approval(s) for some of the information on the system. For systems processing classified information, this means that all users have all required clearance(s) and all required formal access approval(s), but at least one user lacks the need to know for some of the information on the system and the information on the system is at a higher level than Confidential (i.e, the level of concern for confidentiality is medium or high).

d. Systems operating at Protection Level 4 can be of two different kinds. A system must meet the requirements for Protection Level 4 when either:

(1) At least one user lacks at least one required **formal** approval for access to all information on the system. For systems processing classified information, this means that all users have all required clearance(s), but at least one user lacks formal access approval(s) for some of the information on the system, or

(2) At least one user on the system lacks any sort of clearance and the information on the system is classified no higher than Confidential.

e. Systems are operating at Protection Level 5 when at least one user has no clearance and the information on the system is classified no higher than Secret and contains no Sigma 1, 2, 14, or 15 restrictions (i.e., the level of concern for confidentiality is medium).

f. Systems are operating at Protection Level 6 when at least one user has no clearance or at least one user is cleared to a level less than Top Secret and the level of concern for confidentiality is high.

DRAFT

3. Significant Risk Systems. Systems operating at protection levels 5 and 6 present a **significant** risk of the loss of classified information. Systems operating at Protection Level 5 or 6 are not permitted to have unclassified access from a public switched network (i.e. Internet). Systems operating at these levels may operate within a protected environment or have connections that provide for encrypted data to pass over public switched networks. Any connection of these systems to other agencies will require an MOU stating that the system/network being connected is not connected to a system or network with public switched network access capabilities.

4. Substantial Risk Systems. Systems operating at protection level 4 present a **substantial** risk of the loss of the separation and need-to-know protection provided by compartmentation. DAAs shall recognize the technical risk of operating such systems.

11/1/96

5. Special Categories. There are several categories of systems that can be adequately secured without implementation of all the technical features specified in Chapter XI. These systems are NOT "exceptions" or "special cases" of the protection levels specified in this Chapter. However, applying the technical security requirements specified in Chapter XI to these systems by rote results in unnecessary costs and operational impacts. In general, the technical question is where, when, and how to apply a given set of safeguards, rather than whether or not to apply the safeguards. For many of these "special" systems (such as guards, pure servers, tactical, data-acquisition, and embedded systems), the physical security protections for the system provide the required access control, while the application running on the platform provides the required user separation.

a. Pure Servers.

(1) Certain specialized systems, when acting as pure servers in a network, do not fit the protection level criteria and may need fewer technical security countermeasures. These systems have the characteristics listed below:

(a) No user code is present on the system.

(b) Only system administrators and maintainers can access the system.

(c) The system provides non-interactive services to clients (e.g., packet routing or messaging services).

(d) The hardware and/or application providing network services otherwise meets the security requirements of the network.

(e) The risk of attack against the SSS using network communication paths is sufficiently low.

(f) The risk of attack against the SSS using physical access to the system itself is sufficiently low.

DRAFT

(2) The **platform (i.e., hardware and operating system)** on which the guard or pure server runs usually need meet no more than protection level 3 security requirements. The guard or pure server may have a large number of clients (i.e., individuals who use the guard's or server's functional capabilities in a severely constrained way). The guard **application** or server **application**, itself, will have to provide the more-stringent technical protections appropriate for the system's protection level and operational environment. Assurances appropriate to the level of concern for the system shall be implemented.

11/1/96

(3) Systems that **do have general users or do execute general user code** are not "Pure Servers" within the meaning of this section, and so must meet all security requirements specified for their protection level and operational environment.

(4) The term "pure server" is not intended to limit the applicability of this section to systems that have traditionally been referred to as servers. For example, a messaging system that happened to be implemented on a general-purpose computer platform could be accredited under this document and, if such a system meets the specifications in a., above, the system's technical requirements could be categorized by this section.

(5) The above easing of technical security requirements does not imply any relaxation in other security requirements (e.g., physical and communications security requirements), which are determined by the information handled or protected by the system. As stated above, this easing of technical requirements is predicated upon adequate application of physical security and other appropriate security disciplines.

b. Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems. Some

systems are incapable of alteration by users, and are designed and implemented to provide a very limited set of predetermined functions. Certain tactical or so-called "embedded" systems fall into this category, as do some data-acquisition systems, and some other special-purpose systems. These systems also have the characteristics that: first, and most importantly, there are NO GENERAL USERS on the system; and, second, there is NO USER CODE running on the system. If the DAA determines that such a system is sufficiently incapable of alteration, and that the application(s) running on the system provide an adequate level of security, then the system does not have to meet additional security requirements specified for more-general-purpose systems in this document. DAAs and implementors are cautioned to be sure that such systems do, in all operational situations, provide the separation appropriate to the system's protection level.

DRAFT

c. Systems with Group Authenticators.

(1) Many of the security measures specified in this document implicitly include the assumption that the system includes an acceptable level of individual accountability. This is normally assured by the use of unique user identifiers and authenticators. Operationally, the design of some systems necessitates more than one individual using the same identifier/ authenticator combination. Such situations are often referred to as requiring the use of group authenticators.

11/1/96

(2) In general, the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. Group authenticators are used for broader access **after** the use of a unique authenticator for initial identification and authentication.

d. Single-User, Standalone Systems. Extensive technical safeguards are normally inappropriate and inordinately expensive for single-user, standalone systems. DAAs can approve administrative and environmental protections for such systems, in lieu of technical safeguards. Except for systems that operate in a periods processing environment as specified below, systems that have one user at a time, but have a total of more than one user, are multi-user systems, and the DAA shall consider the systems as such in determining the protection level and the resulting security requirements.

e. Periods Processing. Periods processing is a method of sequential operation of an information system that provides the capability to process various levels of sensitivity of information at distinctly different times. Periods processing provides the capability to either: (a) have more than one user (sequentially) on a single-user information system with different levels of information or need-to-

know; (b) use an information system at more than one protection level (sequentially); or © use an information system in more than one protection level at the same time.

(1) Sanitization After Use. If an information system is used for periods processing either by more than one user or for segregating information by classification level onto separate media, the SSP shall specify the sanitization procedures to be employed by each user before and after each session of use of the system.

(2) Sanitization Between Periods. The information system shall be sanitized of all information before transitioning from one period to the next (e.g., whenever there will be a new user(s) who does not have security clearance or the need-to-know for data processed during the previous period, changing from one protection level to another). These procedures shall be documented in the SSP and approved by the DAA. Such procedures could include, among others, sanitizing nonvolatile storage, exchanging disks, and powering down the information system and its peripherals.

(3) Media For Each Period. Information systems employed in periods processing shall have separate media for each period of processing, including copies of operating systems, utilities, and applications software.

(4) Audit. Where there are multiple users of the system and where the system is not capable of automated logging, manual logging shall be done at the discretion of the DAA. Audit trails are not required for single-user standalone systems.

DRAFT
11/1/96

6. **Protection Level Table for Confidentiality**

Level of Concern	Lowest Clearance	Formal Access Approval	Need To Know	Protection Level
High	Uncleared or less than Top Secret	NOT ALL Users Have ALL	NOT ALL Users Have ALL	6
Medium	Uncleared	NOT ALL Users Have ALL	NOT ALL Users Have ALL	5
Low	Uncleared	NOT ALL Users Have ALL	NOT ALL Users Have ALL	4
High, Medium, or Low	At Least Equal to Highest Data	NOT ALL Users Have ALL	NOT ALL Users Have ALL	4
High or Medium	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	3
Low	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	2
High, Medium, or Low	At Least Equal to Highest Data	ALL Users Have ALL	ALL Users Have ALL	1

DRAFT 11/1/96

CHAPTER X

BASELINE REQUIREMENTS

1. Introduction. This chapter describes the implementation requirements that are common to all systems.

2. Clearing and Sanitization.

   a. Clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information. Detailed instructions on clearing shall be issued periodically by the ISPM.

   b. Sanitization. Sanitization of a classified AIS resource shall be accomplished before it may be released from classified information controls or released for use at a lower classification level. To sanitize storage media, memory, and hardware, follow the guidance issued periodically by the ISPM.

   c. Visual Examination of Hardware Components. To complete sanitization of a Classified AIS, any classified media such as diskettes, disk cartridges, disks, tapes, printer ribbons, and hardcopy output shall be physically removed. An examination of the display device for evidence of residual information shall be conducted.

3. Examination of Hardware and Software. Information Systems hardware and software shall be examined when received from the vendor and before being placed into use.

   a. Information Systems Software. Commercially procured software shall be tested to assure that the software contains no obvious features which might be detrimental to the security of the information system. Security related software shall be tested to assure that the security features function as specified.

   b. Information Systems Hardware. An examination shall result in assurance that the equipment appears to be in good working order and has no "parts" that might be detrimental to the secure operation of the information system when placed under site control and cognizance. Subsequent changes and developments which affect security may require additional examination.

DRAFT
11/1/96

4. Identification and Authentication Management. Identification and authentication is required to ensure that users are associated with the proper security attributes, such as, identity, protection level, or location. Controls, such as biometrics or smart cards may be used at the discretion of the ISSO with approval of the ISSM and DAA.

a. Identifier Management. User identifiers shall be managed in accordance with procedures identified in the SISP.

b. Authenticator Management. User authenticators shall be managed in accordance with procedures identified in the SISP.

c. Unique Identification. Each user shall be uniquely identified and that identity shall be associated with all auditable actions taken by that individual.

d. Authentication at Login. Users shall be required to authenticate their identities at "logon" time by supplying their authenticator, such as, a password, smart card, or biometrics, in conjunction with their user ID prior to the execution of any application or utility on the system.

e. Access to Authentication Data. Access to authentication data shall be restricted to authorized personnel through the use of encryption or file access controls, or both.

f. User ID Reuse. Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) shall be removed from the system.

g. User ID Removal. Ensure that a user ID and its authentication shall be removed or disabled from the system (e.g., when an employee leaves the sponsoring organization, when notified of the need to remove access for cause).

h. User ID Revalidation. The ISSO shall ensure that all active user IDs are revalidated at least annually, and information such as sponsor and means of offline contact (e.g., phone number, mailing address) are updated as necessary.

i. Protection of Authenticator. An authenticator that is in the form of knowledge or possession (password, smart card, keys,) shall not be shared with anyone.

j. Protection of Passwords. When passwords are used as authenticators:

(1) They shall be protected at a level commensurate with the sensitivity level or classification level and classification category of the information to which they allow access.

(2) They shall contain a minimum of six nonblank characters.

DRAFT 11/1/96

(3) They shall be produced by a method approved by the DAA. In no case shall a user "supply" his/her own password. Password acceptability shall be based on the method of selection, the length of password, and the size of the password space. The password selection method, the length of the password, and the size of the password space shall be described in an attachment to the SSP.

(4) When an information system cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask shall be printed before the password is entered to conceal the typed password.

(5) User software including operating system and other security-relevant software comes with a few standard authenticators (e.g., SYSTEM, TEST, MASTER) and passwords already enrolled in the system. The ISSO shall ensure that the passwords for all standard authenticators are changed before allowing the general user population access to the information system. The ISSO shall also ensure that these passwords are changed after a new system release is installed or after other action is taken that might result in the restoration of these standard passwords.

(6) If the level of concern for confidentiality is low, the lifetime of a password shall not exceed 12 months. If the level of concern is medium or high, the lifetime of a password shall not exceed 6 months.

DRAFT 11/1/96

5. Maintenance. Information systems are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified and unclassified information and facilities.

a. Cleared Maintenance Personnel. Personnel who perform maintenance on systems shall be cleared to the highest classification level of information on the system, and indoctrinated for all information processed on that system. Cleared personnel who perform maintenance or diagnostics on information systems do not require an escort. However, when possible, an appropriately-cleared and technically-knowledgeable, facility employee shall be present within the area where the maintenance is being performed to assure that the proper security and safety procedures are being followed.

b. Uncleared (or lower-cleared) Maintenance Personnel.

(1) If appropriately-cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used provided a fully-cleared and technically-qualified escort monitors and records their activities in a maintenance log.

(2) Uncleared maintenance personnel who are not U.S. citizens shall have Initiation and Termination performed by the fully-cleared and technically-qualified escort. In addition keystroke monitoring shall be performed during their access to the system.

(3) Prior to maintenance by uncleared personnel, the information system shall be completely cleared and all nonvolatile data storage media removed or physically disconnected and secured. When a system cannot be cleared, ISSM-approved procedures shall be enforced to deny the uncleared individual visual and electronic access to any classified or sensitive data that is contained on the system.

DRAFT

(4) A separate, unclassified copy of the operating system, including any micro-coded floppy disks or cassettes that are integral to the operating system, shall be used for all maintenance operations performed by uncleared personnel. The copy shall be labeled "UNCLASSIFIED -- FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSP. Maintenance procedures for an information system using a non-removable storage device on which the operating system is resident shall be considered by the ISSM on a case-by-case basis.

c. General Maintenance Requirements.

11/1/96

(1) A maintenance log shall be maintained. The maintenance log shall include the date and time of maintenance, name of the individual performing the maintenance, name of escort, and a description of the type of maintenance performed, to include identification of replacement parts.

(2) Maintenance of systems shall be performed on-site whenever possible. Equipment repaired off-site and intended for reintroduction into a facility may require protection from association with that particular facility or program.

(3) If systems or system components shall be removed from the facility for repair, they shall first be purged, and downgraded to an appropriate level, or sanitized of all classified data and declassified in accordance with ISSM-approved procedures. The ISSO shall approve the release of all systems and all parts removed from the system.

(4) Introduction of network analyzers (e.g., sniffers) that would allow the maintenance personnel the capability to do keystroke monitoring shall be approved by the ISSM prior to being introduced into an information system.

(5) If maintenance personnel bring diagnostic test programs (e.g., software/ firmware used for maintenance or diagnostics) into a facility, the media containing the programs shall be checked for malicious codes before the media is connected to the system, shall remain within the facility, and shall be stored and controlled at the level of the information system. Prior to entering the facility, the maintenance personnel shall be advised that they shall not be allowed to remove media from the facility. If deviation from this procedure is required under special circumstances, then each time the diagnostic test media is introduced into a facility, the media shall undergo stringent integrity checks (e.g., virus scanning, checksum, etc.) prior to being used on the information system and, before leaving the facility, the media shall be checked to assure that no classified information has been written on the media. Such a deviation shall be approved by the ISSM.

DRAFT

(6) All diagnostic equipment and other devices carried into a facility by maintenance personnel shall be handled as follows:

(a) Systems and system components being brought into the facility shall be inspected for improper modification.

(b) Maintenance equipment that has the capability of retaining information shall be appropriately sanitized by procedures outlined in Appendix D before being released. If the equipment cannot be sanitized, the equipment shall remain within the facility, be destroyed, or be released under procedures approved by the DAA and the data owner(s) or responsible official(s).

11/1/96

(c) Replacement components that are brought into the facility for the purpose of swapping with facility components are allowed. However, any component placed into an information system shall remain in the facility until proper release procedures are completed. Any component that is not placed in an information system may be released from the facility.

(d) Communication devices with transmit capability (e.g., pagers, RF LAN connections, etc.) belonging to the maintenance personnel or any data storage media not required for the maintenance visit shall remain outside the system facility for return to the maintenance personnel upon departure from the facility.

(7) Maintenance changes that impact the security of the system shall receive a configuration management review.

(8) After maintenance has been performed, the security features on the information systems shall be checked to assure that they are still functioning properly.

d. Remote Maintenance.

(1) Remote Diagnostic Maintenance service may be provided by a service or organization that **does** provide the same level and category(ies) of security. The communications links connecting the components of the systems, associated data communications, and networks shall be protected in accordance with national policies and procedures applicable to the sensitivity level of the data being transmitted.

DRAFT

(2) If remote diagnostic or maintenance services are required from a service or organization that **does not** provide the same level of security required for the system being maintained, the information system shall be sanitized and in a stand-alone mode prior to the connection of the remote access line. If the system cannot be sanitized (e.g., due to a system crash), remote diagnostic and maintenance shall not be allowed. Initiation and termination of the remote access shall be performed by the ISSO. Keystroke monitoring shall be performed on all remote diagnostic or maintenance services. A technically qualified person shall review the maintenance log to assure the detection of unauthorized changes. The ISSO shall assure that maintenance technicians responsible for performing remote diagnosis/ maintenance are advised (contractually, verbally, banner, etc.) prior to remote diagnostics/maintenance activities that keystroke monitoring shall be performed. Maintenance personnel accessing the information systems at the remote site shall be cleared to the highest level of information processed on that system prior to sanitization. Installation and use of remote diagnostic links shall be addressed in the SSP. An audit log shall be maintained of all remote maintenance, diagnostic, and service transactions and periodically reviewed by the ISSO. Other techniques to consider include encryption and decryption of diagnostic communications, strong identification and authentication techniques, such as tokens, and remote disconnect verification.

11/1/96

(3) System maintenance requirements and vulnerabilities shall be addressed during all phases of the system life cycle. Specifically, contract negotiations shall consider the security implications of system maintenance.

6. Malicious Code.

a. Site Policies. Policies and procedures, identified in the SISP, to detect and deter

incidents caused by malicious code, such as viruses, or unauthorized modification to software shall be implemented.

b. Personal Software. The use of software purchased or developed by an individual for personal use on an information system is discouraged. If such software is required or desired to enhance the information system operation, each installation of the software shall be approved by the ISSM.

c. Public Domain Software. The use of public domain software on an information system is strongly discouraged. Procedures, identified in the SISP, to carefully examine this software for malicious code before it is introduced into the information system environment shall be implemented.

d. Review of Security-Relevant Changes. All modifications to security-relevant resources (including software, firmware, hardware, or interfaces and interconnections to networks) shall be reviewed and approved in accordance with procedures identified in the SISP prior to implementation. All security-relevant modifications shall be subject to the provisions of the system configuration management program. The ISSM shall notify the DAA of requests for changes to the resources that deviate from the requirements of the approved SSP. The DAA shall consider the system for reaccreditation.

7. Marking Hardware, Output, and Media. Markings on hardware, output, and media shall conform to guidelines issued by the cognizant ISPM. If the marking required by the guidelines is impractical or interferes with the operation of the media, the DAA may approve alternate marking procedures. The alternate marking procedures shall be documented.

a. Hardware Components. Procedures identified in the SISP shall be implemented to ensure that all components of an information system, including input/output devices, terminals, standalone microprocessors, or word processors used as terminals, bear a conspicuous, external label which states the highest classification level and most restrictive classification category of the information accessible to the component in the information system. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the information system and displayed on the screen.

b. Hardcopy Output. Hardcopy output includes paper, fiche, film, and other printed media. The accreditation level of the accredited information system shall be marked on all hardcopy output that is retained in, or distributed from, the facility unless an appropriate classification review has been conducted or the information has been output by a tested program verified to produce consistent results and approved by the DAA. Such programs will be tested on a statistical basis to

DRAFT 11/1/96

assure continuing performance.

c. Removable Media. Procedures identified in the SISP shall be implemented by the ISSO to ensure that personnel handling removable media apply visible, human-readable, external markings to the media. Removable media shall be marked with the accreditation level of the information system unless an appropriate classification review has been conducted or the information on the media has been outputted by a tested program or methodology verified to produce consistent results and approved by the DAA.

d. Unclassified Media. In facilities where some of the information systems are operated as classified and some are dedicated to unclassified operation, the removable unclassified media shall be uniquely marked to protect from the mixing of the media.

DRAFT

8. Personnel Security. Personnel play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their information-processing systems. Personnel directly involved with a system may be users, operators, administrators, COMSEC custodians, and installers/maintainers. Duties, responsibilities, privileges, and specific limitations of information systems users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system.

11/1/96

a. Access Approvals. Background investigations of applicants, employees, contractors, and other individuals shall be performed as necessary to meet appropriate standards -- for access to classified information, the appropriate standards are national standards.

(1) For systems that process classified information at Protection Level 1, 2, or 3, individuals shall be **cleared** to the highest level of classification processed on that system. For Protection Level 4, 5, or 6 systems, the individual need only to be **cleared** for the information to which they are allowed access.

(2) For Protection Level 1, 2, or 3 systems, the individuals shall have all required formal access approval(s) for all information on the systems. For Protection Level 4, 5, or 6 systems, the individuals need formal access approval for only that information to which they are allowed access.

b. General Users.

(1) General Users shall:

(a) Access only that data, control information, and software for which they are authorized access and have a need to know.

(b) Immediately report all security incidents and potential threats and vulnerabilities involving information systems to the appropriate ISSO.

(c) Protect their authenticators and report any compromise or suspected compromise of an authenticator to the appropriate ISSO.

(d) Assure that system media and system output is properly classified, marked, controlled, and stored.

(e) Protect terminals from unauthorized access.

(f) Inform the ISSO when access to a particular information system is no longer required (e.g., completion of project, transfer, retirement, resignation, etc.).

(g) Observe rules and regulations governing the secure operation and authorized use of information systems.

(h) Use the information system only for official government business.

(2) General Users shall not attempt to:

(a) Introduce malicious code into any information system or physically damage the system.

(b) Bypass, strain, or test security mechanisms. If security mechanisms must be bypassed for any reason, users shall coordinate the procedure with the ISSO, and receive written permission from the ISSM for the procedure.

(c) Introduce or use unauthorized software, firmware, or hardware on an information system.

(d) Assume the roles and privileges of others and attempt to gain access to information for which they have no authorization.

(e) Relocate information system equipment without proper authorization.

c. Privileged Users:

DRAFT 11/1/96

(1) The number of privileged users shall be limited to the absolute number needed to manage the system.

(2) Examples of privileged users (for multi-user systems) include:

(a) Users having "super-user", "root", or equivalent access to a system (i.e., system administrators, computer operators, perhaps system security officers, etc.). Those individuals who have near or complete control of the operating system of the machine or information system or who set up and administer user accounts, authenticators, and the like.

(b) Users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexors, and other key information system equipment.

(c) Users who have been given the power to control and change other user's access to data or program files (i.e., applications software administrators, administrators of specialty file systems, database managers, etc.).

(d) Users who have been given special access for troubleshooting of information systems/security monitoring functions (i.e., those using information system analyzers, management tools, etc.).

DRAFT 11/1/96

(3) All privileged users shall be responsible for all the requirements as stated for general users.

(4) Privileged users shall:

(a) Be U.S. citizens unless approved in writing by the DAA.

(b) Possess access approvals to all the information on the system; and possess clearance equal to the highest classification of data processed on or maintained by the information system.

(c) Protect the root or superuser authenticator at the highest level of data it secures and not share the authenticator and/or account.

(d) Be responsible for all superuser or root actions under his/her account.

(e) Report any and all information system problems to the ISSO.

(f) Use special access or privileges granted only to perform authorized tasks and functions.

(5) Privileged users shall not:

(a) Enroll any unauthorized user on an information system.

(b) Use special access or privileges to perform unauthorized tasks or functions.

9. Physical Security.

a. Protection. The information and system shall be located in a area appropriate to the classification and sensitivity of the data.

b. Visual Access. Devices which display or output information in human-readable form shall be positioned to deter unauthorized individuals from reading the information without the knowledge of the user.

c. Information Protection. Information shall be protected by the use of DAA-approved procedures to prohibit unauthorized use of communications lines and other system resources, and at least one of the following:

(1) The information is continuously attended by properly authorized personnel, or

(2) The information is locked in GSA-Approved containers when not attended, or

(3) During normal work periods, the information is protected by day locks, as defined in Departmental directives, or

(4) The system is sanitized as described in guidelines issued by the ISPM, or

(5) The information is located in an area approved for open storage of the information.

d. Unescorted Access. All personnel granted unescorted physical access to the system or information shall have a need to know for all information in the area or on the information system.

10. Protection of Media.

a. Media Protection. Media must be protected by at least one (or a combination) of

DRAFT 11/1/96

the following until the media has been reviewed following a DAA or DAA-approved procedure.

(1) Storage in an area approved for open storage of information at the accreditation level of the information system, or

(2) Storage in an area approved for open storage of information at the accreditation level of the information system while continuously attended, if the area is continuously attended, or

(3) Type 1 encryption of stored data, or

(4) GSA-Approved Container.

DRAFT

b. Removable Media. Removable media shall be controlled and protected in a manner similar to that used for classified paper materials.

c. Laser Printers.

(1) Property Protection Area. If the laser printer is located in a property protection area approved for classified processing, the toner cartridge shall be sanitized at the end of the session using DAA-approved procedures or the toner cartridge shall be removed from the printer and stored in a container approved for the storage of classified materials.

11/1/96

(2) Limited Area. If the laser printer is located in a limited area, the toner cartridge is protected while it is in the printer. If the toner cartridge must be removed from the printer, the toner cartridge shall be stored in a container approved for the storage of information on the system; or the toner cartridge shall be sanitized using DAA-approved procedures.

(3) Open Storage Area. If the laser printer is located in an area approved for the open storage of the information, the toner cartridge does not require additional protection while in the printer. If the toner cartridge must be removed from the printer, the toner cartridge shall be stored in a container approved for the storage for classified materials; or the toner cartridge shall be sanitized using DAA-approved procedures.

11. Review of Output.

a. Human-readable Output Review. An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the system boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

b. Media Review. Electronic output, such as files, to be released outside the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content with the appropriate software application. Random or representative sampling techniques may be used to verify the proper marking of large volumes of output. The media sampling procedures shall be defined and documented. DAA-approved automated techniques may be used to verify the proper marking of output.

DRAFT

11/1/96

DRAFT

(Page Intentially Left Blank)

11/1/96

CHAPTER XI

PROTECTION REQUIREMENTS

1. Introduction. Each section of this chapter describes the implementation requirements for a different protection measure.

2. Alternative Power Source. An alternate power source ensures that the system availability is maintained in the event of a loss of primary power. An alternate power source can also provide a time period for orderly system shutdown or the transfer of system operations to another system or power source.

DRAFT

a. APS-1 Requirements.

(1) Alternative Power Source. The decision to not use an alternative source of power, such as an uninterruptible power supply (UPS) for the system shall be documented.

b. APS-2 Requirements. Instead of APS-1

(2) Alternative Power Source. Procedures for the graceful shut-down of the system shall ensure that there is no loss of data.

11/1/96

c. APS-3 Requirements. Instead of APS-2

(3) Alternative Power Source. Procedures for transfer of the system to another power source shall ensure that the transfer is completed within the time requirements of the application(s) on the system.

d. Profile requirements:

Requirements			
Availability	Low	Medium	High
Alternative Power Source	APS-1	APS-2	APS-3

3. Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security relevant activities. The audit records can be used to determine which activities occurred and which user was responsible for them.

a. AUD-1 Requirements.

(1) Audit Trail Creation. The system shall automatically create and maintain an audit trail or log that includes records of:

Successful and unsuccessful logons and logoffs.

For each recorded event, the audit record shall contain, at a minimum, the date and time of event, the user ID, the type of event, and the success or failure of the event.

DRAFT

(2) Audit Trail Protection. The contents of audit trails shall be protected against unauthorized access, modification, or deletion.

(3) Audit Trail Analysis. Audit analysis and reporting shall be scheduled, performed, and documented on a regular basis. The frequency of the review shall be documented in an attachment to the SSP.

(4) Audit Record Retention. Audit records shall be retained for at least 6 months.

11/1/96

(5) Alternative Methods. Where it is not possible to provide an automated audit trail or log, an alternative method of accountability for user activities on the system shall be developed and documented.

b. AUD-2 Requirements. In addition to AUD-1:

(1) Audit Trail Creation. In addition to the Audit Trail Creation requirement in AUD-1, the system shall automatically create and maintain an audit trail that includes records of:

- Privileged activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.
- Successful and unsuccessful accesses to security-relevant files, including creation, open, close, modification, and deletes.
- Starting and ending times of each access to the system.
- Changes in user authenticators.
- The blocking or blacklisting of a user ID, terminal, or access port and the reason for the action.
- Denial of access resulting from an excessive number of unsuccessful

logon attempts.

For each recorded event, the audit record shall contain, at a minimum, the date and time of event, the user ID, the type of event, and the success or failure of the event.

(6) Audit Failure. Procedures shall be implemented to ensure alternate audit capability or system shutdown in the event of audit failure.

c. AUD-3 Requirements. In addition to AUD-2:

(7) Automated Audit Analysis. Audit analysis and reporting using automated tools shall be scheduled and performed.

(8) Security Label Changes. The system shall automatically record the creation, deletion, or changes in security labels.

d. AUD-4 Requirements. In addition to AUD-3:

(9) Continuous Monitoring. Auditing shall include the continuous, online monitoring of auditable events. The system shall notify an authorized person when imminent violations of security policies are detected.

e. Profile requirements:

DRAFT 11/1/96

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Audit Capability	AUD-1	AUD-1	AUD-2	AUD-3	AUD-4	AUD-4

Requirements			
Integrity	Low	Medium	High
Audit Capability	AUD-1	AUD-2	AUD-4

4. Backup and Restoration of Data. The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.

a. BRD-1 Requirements.

(1) Backup Procedures. Procedures for the regular backup of all essential and security-relevant information, including software tables and settings, such as router tables, software, and documentation on a regular basis shall be documented.

(2) Backup Frequency. The frequency of backups shall be defined by the ISSO, with the assistance of the data owner(s), and documented in the backup procedures.

b. BRD-2 Requirements. In addition to BRD-1:

(3) Backup Media Storage. Media containing backup files and backup documentation shall be stored at another location, such as another part of the same building, a nearby building, or offsite, in such a way to reduce the possibility that a common occurrence could eliminate the on-site data backup data and the off-site backup data.

(4) Verification of Backup Procedures. Backup procedures shall be periodically verified by confirming that the date of last backup is consistent with the backup procedures.

c. BRD-3 Requirements. In addition to BRD-2:

(5) Information Restoration Testing. Complete restoration of information from backup media shall be tested on a periodic basis. The frequency of restoration testing shall be defined and documented in the backup procedures.

DRAFT 11/1/96

d. Profile requirements:

Requirements			
Availability	Low	Medium	High
Backup and Restoration of Data	BRD-1	BRD-2	BRD-3

5. Changes to Data. The control of changes to data includes the deterring, detecting, and reporting of successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to the ability to ensure that only authorized changes are allowed.

a. CD-1 Requirements.

(1) Change Procedures. Procedures and technical system features shall be implemented to ensure that changes to the data are executed only by authorized personnel or processes.

b. CD-2 Requirements. In addition to CD-1:

(2) Transaction Log. A transaction log, protected from unauthorized changes, shall be available to allow the immediate correction of unauthorized data changes, and the off-line verification of all changes at all times.

c. Profile requirements:

DRAFT

Requirements			
Integrity	Low	Medium	High
Changes to Data	CD-1	CD-1	CD-2

6. Communications. Information protection is required whenever National Defense (classified or any of the special categories of unclassified information under the security cognizance of NN) information is to be transmitted or carried to, or through, areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).

11/1/96

a. COM-1 Requirements.

(1) Protections. One or more of the following protections shall be used:

(a) Information distributed only within an area approved for open storage of the information, or

(b) NSA-approved encryption mechanisms appropriate for the encryption of classified information, or

(c) NIST-approved encryption mechanisms appropriate for the encryption of unclassified information, or

(d) Protected Distribution System, or

(e) Trusted Courier.

(2) Unauthorized Use of Communications Lines. All interfaces to Protected Distribution Systems shall be disconnected and shall be secured (both the

disconnection and securing of the interface shall be accomplished with a DAA-approved mechanism).

b. COM-2 Requirements. In addition to COM-1:

(3) Public Switched Networks. Any classified system connected to a public switched network (e.g. Internet) or an internal network that is not accredited at the same level must utilize a Controlled Interface that meets the requirements in Chapter VI and performs the following:

(a) Review Before Release. Unclassified communication from the inside shall be reviewed for classification before being released.

(b) Encryption of Message Body. The body of classified communication from the inside shall be encrypted with NSA-approved encryption mechanisms appropriate for the classification of the information for encryption of stored data.

(c) Notification of Recipient. Communication from the outside must have an inside sponsor (i.e. the CI will notify the sponsor of the communication and release the communication on notification from the sponsor).

(d) Review of Outside Communications. Communication from the outside shall be reviewed for viruses and other malicious code.

DRAFT 11/1/96

(4) End-to-end Integrity. Integrity attributes adequate to assure the end-to-end integrity of transmitted information (including labels and security parameters) shall be included with all information that is transmitted externally to a system or network.

c. Profile requirements:

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Communications	COM-1	COM-1	COM-1	COM-2	COM-1	COM-1

NOTE: The Department of Energy will not approve systems at PL 5 or PL 6 to be attached to public switched networks.

Requirements			
Integrity	Low	Medium	High
Communications	COM-1	COM-1	COM-2

7. Configuration Management. Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.

DRAFT

a. CM-1 Requirements.

(1) Configuration Documentation. Procedures for identifying and documenting the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security-relevant software product names and version or release numbers, and physical location shall be implemented.

(2) System Connectivity. Procedures for identifying and documenting system connectivity, including any software used for wireless communication, and any communications media shall be implemented.

11/1/96

b. CM-2 Requirements. In addition to CM-1:

(3) Connection Sensitivity. The sensitivity level of each connection or port controlled by the Security Support Structure (SSS) shall be documented.

(4) CM Plan. The CM plan shall be documented. The CM plan shall include:

(a) Formal change control procedures for security-relevant hardware and software.

(b) Procedures for management of all documentation, such as the Systems Security Plan (SSP) and security test plans, used to ensure system security.

(c) Workable processes to implement, periodically test, and verify the plan.

c. CM-3 Requirements. In addition to CM-2:

(4) CM Plan. In addition to the requirements of CM plan in CM-2, the CM plan shall include:

(d) A CM control board that implements procedures identified in the SISP to ensure the security review and approval of changes that affect the SSS.

(e) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

d. Profile requirements:

DRAFT

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Configuration Management	CM-1	CM-1	CM-1	CM-2	CM-3	CM-3

Requirements			
Integrity	Low	Medium	High
Configuration Management	CM-1	CM-2	CM-3

11/1/96

8. Disaster Recovery Planning.

a. DRP-1 Requirements.

(1) Mission Essential. Identification of the site's Mission-Essential Applications and Development of Descriptions of Each Mission Essential Application.

(2) Plan Decision. A decision concerning the need for a continuity of operations plan or contingency plan for each information system shall be made by the manager or supervisor directly responsible for the system. This decision shall be documented and signed by the manager or supervisor. A statement of the decision and the basis for that decision shall be documented in the SSP. If a continuity of operations plan or contingency plan is not needed, a statement to that effect shall be included in the SSP.

(3) Procedures. Documented procedures for the backup of all essential information, software and documentation on a regular basis shall be implemented. The backup procedures shall be attached to or referenced in an attachment to the SSP. The frequency of backups shall be defined by the ISSO, with the assistance of the data owner(s), and documented in the backup procedures.

(4) Plan Elements. The elements of a disaster recovery plan defined in MA-365, "Disaster Recovery Program Guideline", dated 7-91, shall be addressed in the plan(s).

b. DRP-2 Requirements. In addition to DRP-1:

(5) Verification of Procedures. Backup procedures shall be periodically verified by confirming that the date of last backup is consistent with the backup procedures. The frequency of verification shall be defined by the ISSO, with the assistance of the data owner(s), and documented in the backup procedures.

c. DRP-3 Requirements. In addition to DRP-2:

(6) Testing of the Disaster Recovery Program. A testing plan shall be developed that addresses the criteria for evaluating the test results and the schedule for performing the tests.

DRAFT 11/1/96

d. Profile requirements:

Requirements			
Availability	Low	Medium	High
Disaster Recovery Planning	DRP-1	DRP-2	DRP-3

9. Independent Validation and Verification.

a. IVV-1 Requirements.

(1) IV&V Team. An Independent Validation and Verification (IV&V) team, in coordination with the ISSM, shall:

(a) assist in the design phase of the system,

(b) assist in determining and developing the certification test

requirements,

(c) assist in the certification testing, and

(d) evaluate the security of the implemented system.

(2) IV&V Request. The request for an IV&V team shall be forwarded through the DAA to the ISPM by the ISSM. The request shall identify funding sources for the IV&V team.

b. Profile requirements:

DRAFT

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Independent Validation and Verification					IVV-1	IVV-1

10. Resource Access Controls. Information Systems shall store and preserve the integrity of the sensitivity of all information internal to the Information System.

a. RAC-1 Requirements.

11/1/96

(1) Discretionary Access Controls. Discretionary access controls shall be provided.

b. RAC-2 Requirements. In addition to RAC-1:

(2) Security Labels. The Information System shall place electronic security labels on all entities (e.g., files) reflecting the sensitivity (classification level, classification category, and handling caveats) of the information for resources and the authorizations (security clearances, need-to-know, formal access approvals) for users. These labels shall be an integral part of the electronic data or media, and shall be compared to the user or resource profile and validated before a user or resource is granted access to the entity.

(3) Export of Security Labels. Security labels exported from the Information System shall be accurate representations of the corresponding security labels on the information in the originating Information System.

(4) Security Label Integrity. The information system shall ensure the following:

(a) Integrity of the security labels;

(b) The association of a security label with the transmitted data; and

(c) Enforcement of the control features of the security labels.

c. RAC-3 Requirements. In addition to RAC-2:

(5) Device Labels. The information system shall ensure that the originating and destination device labels are a part of each message header and enforce the control features of the data flow between originator and destination.

(6) Mandatory Access Controls. Mandatory access controls shall be provided.

d. Profile requirements:

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Resource Access Control		RAC-1	RAC-1	RAC-2	RAC-3	RAC-3

11. Resource Utilization.

a. RU-1 Requirements.

(1) Resource Reallocation. The system shall ensure that resources contain no residual data before being assigned, allocated, or reallocated.

b. RU-2 Requirements. In addition to RU-1:

(2) Resource Allocation. The Security Support Structure shall provide the capability to control a defined set of system resources (e.g., memory, disk space) such that no one user can deny another user access to the resources.

DRAFT 11/1/96

c. Profile requirements:

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Resource Utilization		RU-1	RU-1	RU-2	RU-2	RU-2

12. Session Controls. Session controls are requirements, over and above, identification and authentication, for controlling the establishment of a user's session.

a. SC-1 Requirements.

DRAFT

(1) User Notification. All authorized information system users shall be notified prior to gaining access to a system that system usage is monitored, recorded, and subject to audit. The user shall also be advised that using the system grants the consent of the user to such monitoring and recording and that unauthorized use is prohibited and subject to criminal and civil penalties. Where the operating system permits, each initial screen (displayed before user logon) shall contain a warning text to the user. The following is a suggested warning text to the user. The user shall be required to take positive action to remove the notice from the screen. Monitoring and recording, such as collection and analysis of audit trail information, shall be performed.

11/1/96

"WARNING: To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this system is prohibited and could be subject to criminal and civil penalties.'

Where it is not possible to provide an "initial screen" warning notice, other methods of notification shall be developed and approved by the DAA.

(2) Successive Login Attempts. Where the operating system provides the capability, successive logon attempts shall be controlled by denying access after multiple (maximum of five) consecutive unsuccessful attempts on the same user ID; by limiting the number of access attempts in a specified time period; by the use of a time delay control system; or other such methods, subject to approval by the DAA.

(3) System Entry. The system shall grant system entry only in accordance

with the conditions associated with the authenticated user's profile. If no explicit entry conditions are defined, the default shall prohibit all remote activities, such as remote logons and anonymous file access.

b. SC-2 Requirements. In addition to SC-1:

(4) Multiple Login Control. If the information system supports multiple login sessions for each user identifier or account, the information system shall provide a protected capability to control the number of login sessions for each user identifier, account, or specific port of entry. The information system default shall be a single login session.

(5) User Inactivity. The information system shall detect an interval of user inactivity, such as no keyboard entries, and disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements shall be documented in the SSP.

(6) Logon Notification. Where the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user's last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

DRAFT 11/1/96

c. SC-3 Requirements. In addition to SC-2:

(7) Security Level Changes. The information system shall immediately notify the user of each change in the security level or compartment associated with that user during an interactive session. A user shall be able to query the information system as desired for a display of the user's complete sensitivity label.

d. Profile requirements:

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Session Controls	SC-1	SC-2	SC-2	SC-3	SC-3	SC-3

13. Security Documentation. Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The Systems Security Plan (SSP) is the basic

system protection document and evidence that the proposed system, or update to an existing system, meets the Protection Profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system.

Common Documents. Information common to several systems at a site or information contained in other documents may be attached to or referenced in the SSP.

a. SD-1 Requirements.

(1) SSP. The SSP shall contain the following:

DRAFT

(a) System Identification.

(i) Security Personnel. The name, location, and phone number of the responsible system owner, DAA, ISSM, and ISSO.

(ii) Description. A brief narrative description of the system or network mission or purpose and architecture, including subnetworks, communications devices, and protocols.

(b) System Requirements Specification.

11/1/96

(i) Sensitivity or Classification Levels of Information. The sensitivity or classification levels and categories of all information on the system.

(ii) Levels of Concern for Confidentiality, Integrity, and Availability. The confidentiality level of concern and protection level, the integrity level of concern, and the availability level of concern.

(iii) Variances from the Protection Profile Requirements. A description of any approved deviations from the Protection Profile. A copy of the approval documentation shall be attached to the SSP.

(c) System Specific Risks and Vulnerabilities. A description of the risk assessment of any threats or vulnerabilities unique to the system. If there are no threats or vulnerabilities unique to the site or system, a statement to that effect shall be entered. If any vulnerabilities are identified by the assessment of unique threats, the countermeasures implemented to mitigate the vulnerabilities

shall be described.

(d) System Configuration. A brief description of the system architecture, including a block diagram of the components that show the interconnections between the components and any connections to other systems.

(e) Connections to Separately Accredited Networks and Systems. If connections to other systems exist, a memorandum of understanding is necessary if the systems are approved by a person other than the DAA responsible for this system. A copy of any memoranda of understanding with other agencies shall be attached to the SSP.

(f) Security Support Structure. A brief description of the security support structure including all controlled interfaces, their interconnection criteria, and security requirements.

(2) Certification and Accreditation Documentation.

(a) Certification documentation. A Certification statement stating that the system complies with the requirements of the protection level and levels of concern for this system. The statement shall be signed by the responsible system owner or the ISSO.

(b) Accreditation Documentation. Documentation for Accreditation includes the certification statement and a cover letter including a recommendation for DAA approval or disapproval.

b. SD-2 Requirements. In addition to SD-1:

(3) System Implementation of Requirements. A brief description of how the system implements each of the security requirements.

c. SD-3 Requirements In addition to SD-2:

(4) Certification and Accreditation Documentation.

(a) Security Testing. Test plans, procedures, and test reports.

(b) Documentation. The test plan for ongoing testing and the frequency of such testing shall be documented in the ISPP.

(c) Compliance Statements. Statements of compliance that

DRAFT 11/1/96

TEMPEST, PDS, and TSCM, and other security requirements have been met.

(d) IV&V Report. Report from the Independent Validation and Verification Team.

d. Profile requirements:

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Security Documentation	SD-1	SD-1	SD-2	SD-2	SD-3	SD-3

DRAFT

14. Separation of Functions.

a. SF-1 Requirements

(1) Separation of Functions. The functions of the ISSO and the system manager shall not be performed by the same person.

b. Profile requirements:

11/1/96

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Separation of Functions				SF-1	SF-1	SF-1

15. System Recovery. System recovery addresses the functions that respond to failures in the SSS or interruptions in operation. Recovery actions ensure that the SSS is returned to a condition where all security-relevant functions are operational or system operation is suspended.

a. SR-1 Requirements.

(1) Controlled Recovery. Procedures and information system features shall be implemented to ensure that information system recovery is done in a controlled manner. If any off-normal conditions arise during recovery, the information system shall be accessible only via terminals monitored by the ISSO, a designated individual, or via the information system console.

b. SR-2 Requirements.

(2) Trusted Recovery. Procedures and technical system features shall be implemented to ensure that system recovery is done in a trusted and secure manner. Procedures to mitigate all information system recovery circumstances where the restoration of protection features cannot be assured shall be implemented and documented in an attachment to the SSP.

c. Profile requirements:

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
System Recovery	SR-1	SR-1	SR-1	SR-1	SR-2	SR-2

DRAFT

16. Security Support Structure. Those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system.

a. SSS-1 Requirements.

(1) Access to Protection Functions. Access to hardware/software/firmware that perform systems or security functions shall be limited to authorized personnel.

11/1/96

b. SSS-2 Requirements. In addition to SSS-1:

(2) SSS Protection Documentation. The protections and provisions of the SSS shall be documented.

(3) Informal Description of Policy Model. An informal description of the security policy model enforced by the SSS shall be documented.

(4) Periodic Validation of SSS. Features and procedures shall exist to periodically validate the correct operation of the hardware, firmware, and software elements of the SSS.

c. SSS-3 Requirements. In addition to SSS-2:

(5) SSS Isolation. The SSS shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modification of its code and data structures).

(6) Policy Description. A description of the security policy model enforced

by the SSS shall be documented with an explanation that shows it is sufficient to enforce the security policy. All interfaces to the SSS shall be included in the explanation.

d. Profile requirements:

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Security Support Structure	SSS-1	SSS-1	SSS-1	SSS-2	SSS-3	SSS-3

Requirements			
Integrity	Low	Medium	High
Security Support Structure	SSS-1	SSS-2	SSS-3

Requirements			
Availability	Low	Medium	High
Security Support Structure	SSS-1	SSS-2	SSS-3

DRAFT 11/1/96

17. Security Testing. Ongoing security testing is the verification of correct operation of the protection measures in a system.

a. ST-1 Requirements.

(1) Verification of Functions. The security functions (e.g., audit trails, system passwords) defined in the PP shall be verified prior to certification by performing tests to confirm correct operation of all security-relevant functions when activated with normal input values.

b. ST-2 Requirements. In addition to ST-1:

(2) Certification Testing. Certification testing shall include the security function verification tests, tests to verify that the security functions do not have any undesired affect(s) on the information system, and tests to verify that the security functions perform correctly when activated with abnormal input values.

(3) Ongoing Testing. Ongoing security performance testing of the system

shall be conducted on a regular basis to ensure that the security features continue to function correctly. The ongoing security performance tests may include all or parts of the security function verification and certification tests. The methods for determining that these features continue to be implemented during the life cycle of the information system (e.g., after system updates) shall be documented.

c. ST-3 Requirements. In addition to ST-2:

(4) Certification Test Reporting. Certification testing provides assurance that the information system is operating in accordance with the approved SSP. The certification test results, when satisfactory, provide the DAA with supporting documentation for the accreditation of the information system.

(a) Certification Test Plans. The ISSO, shall develop the certification test plan to assure that the information system has been implemented and is operating in accordance with the SSP. The certification test plan shall be approved by the DAA. If the security features of the information system, as specified in the SSP, are expected to restrict user access, for example, these features shall be tested to ensure that they are implementing the specified security requirements.

(b) Certification Test Performance. The ISSO shall ensure that the specified tests are performed.

(c) Documentation. The results of certification tests and an analysis of the results shall be documented.

(d) Additional Tests. Following receipt of the certification documentation, the DAA may designate additional tests that shall be performed prior to meeting accreditation requirements.

d. ST-4 Requirements. In addition to ST-3:

(5) Penetration Testing. Ongoing prudent penetration testing shall be performed to identify major or obvious vulnerabilities in the system. The test methodology and procedures shall be described in a security test plan. The ongoing penetration tests may include all or parts of the security function verification tests.

(6) Independent Validation and Verification. An Independent Validation and Verification team shall assist in the certification testing of an information system and shall perform validation testing of the system as required by

DRAFT 11/1/96

the DAA.

e. Profile requirements:

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Security Testing	ST-1	ST-2	ST-2	ST-3	ST-4	ST-4

Requirements			
Integrity	Low	Medium	High
Security Testing	ST-1	ST-3	ST-4

DRAFT

18. Trusted Path. Users often need to perform functions, such as authentication, through direct interaction with the SSS. A trusted path ensures that the user is communicating directly with the SSS. Trusted path exchanges may be initiated by a user or the SSS. A user response via the trusted path guarantees that untrusted processes cannot intercept or modify the user's response.

11/1/96

a. TP-1 Requirements.

(1) Authentication Path. The information system shall support a trusted path between itself and the user for initial identification and authentication.

b. Profile requirements:

Requirements						
Confidentiality	PL 1	PL 2	PL 3	PL 4	PL 5	PL 6
Trusted Path					TP-1	TP-1

ATTACHMENT 1

DEFINITIONS

Accreditation

Accreditation is a formal acknowledgment (written or electronic) of the decision by the designated approval authority to authorize an information system to process, store, transfer, or provide access to information in a specific information systems security environment established by a specific SSP .

Automated Information

Information that is collected, created, processed, transmitted, stored or disseminated by an automated information system.

DRAFT

Availability

The attribute of information being in the place, at the time, and in the form needed by the user. Denotes the goal of ensuring that information and information processing resources both remain readily accessible to their authorized users.

Boundary

The conceptual limit of an information system that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system without a reliable human review by an appropriately authorized or cleared authority.

11/1/96

Classified Information Systems Security Program Manager (ISPM)

The individual responsible for the development of Departmental policies, standards, guidelines, and procedures for the protection of classified information in automated information systems.

Classified Information Systems Security Operations Manager (ISOM)

The technical expert responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an information system.

Classified Information Systems Security Site Manger (ISSM)

The manager responsible for a site information systems security program.

Classified Information Systems Security Officer (ISSO)

The person responsible for ensuring that protection measures are installed and operational security is maintained for one or more specific information system.

Clearance

A clearance is the formal determination that a given individual meets the national clearability standards for access to one or more pieces of information.

Clearing

Removal of data from an information system, its storage media, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using normal system capabilities (i.e., through the keyboard). NOTE: Clearing does not permit the reuse of media at a lower classification level or unclassified if the media has contained classified information.

Confidentiality

The critical attribute of information of being inaccessible except to persons or processes that have an authorization and a legitimate need or right to read that information.

Covered Contractor

A covered contractor (e.g., management and operating contractor, service support contractor, onsite contractor) is a seller of supplies or services that has been awarded a procurement contract or subcontract to provide supplies or services on an information system.

DRAFT

Data Steward

The individual responsible for introducing and managing information on an information system. This person is the "steward" of the information and is responsible for its generation, management, and destruction.

Data Owner

This person declares the sensitivity, classification, category, and dissemination requirements of the information. The person to whom the data belongs.

11/1/96

Designated Approval Authority

Official with the authority to formally grant approval for operating an information system. This person determines the acceptability of the remaining or residual risk in a system that is prepared to process classified information and either accredits or denies operation of the system for the Department.

DOE Office

An Operations or Field Office (including Headquarters).

Formal Access Approval

The formal determination that a specific individual must have access to certain information to accomplish that individual's mission, or to do that individual's job. NOTE: Such access generally requires signing of an appropriate non-disclosure agreement, and entry of the individual's name on an access roster. For intelligence information, formal access approval is indicated by the requirement for signing an "Intelligence Non-Disclosure Agreement."

Information

Facts, data, or knowledge itself, rather than the medium of its conveyance. Documents and material are deemed to convey or contain information and are not considered to be information per se.

Information System

Information systems are defined in NSTISSC 4009, National Information Systems Security (INFOSEC) Glossary, dated 5 June 1992 as "any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware."
NOTE: COMSEC and TSCM Requirements are contained in other Orders.

DRAFT

Integrity

The attribute of information of being a true, complete representation of its original content, even when undergoing changes in form or storage medium..

Level of Concern

An expression of the information's perceived value and the consequences of loss of , integrity, availability, or confidentiality.

Perimeter

The perimeter of a system encompasses all those components of the system that are to be accredited. NOTE: As a rule, separately accredited components are not included within the perimeter; but, those components are within the boundary.

11/1/96

Processing

The state that exists when information is being accessed or acted-upon by one or more steps proceeding in a predetermined sequence or method, such as a program.

Risk

The expected loss from a given attack or incident. Risk is the product of Threat (expressed as the probability that a given attack or incident will occur) times Net Vulnerability (expressed as the probability that the given attack or incident will succeed, given that the attack or incident occurs) times Consequence (expressed as some measure of loss, such as dollar cost, resources cost, programmatic impact, etc.). The total risk of operating a system is the integration of the risks of all possible attack/defense scenarios.

Residual Risk

The remaining risk of operating the system after application of mitigating factors.
NOTE: Such mitigating factors often include, but are not limited to:

- minimizing initial risk by selecting a system known to have fewer vulnerabilities;
- reducing vulnerabilities by implementing countermeasures;

- reducing consequence by limiting the amounts and kinds of information on the system; and
- using classification and compartmentation to lessen threat by limiting the adversaries' knowledge of the system.

Sanitizing

The removal of information from media or equipment such that data recovery using any known technique or analysis is prevented. NOTE: Sanitizing shall include the removal of data from the media, as well as the removal of all sensitivity or classified labels, markings, and activity logs.

Sensitive Unclassified Information

Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or government interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U. S. Government. Government interests are those related, but not limited, to the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law-enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided the U. S. Government by its citizens.

Site

A geographical area where one or more facilities are located. An educational institution, manufacturing plant, laboratory, office building, or complex of buildings located on the same site that is operated and protected as one unit by the Department or its contractor(s).

Site Manager

The Director or manager of a site. This individual is the person responsible for management of all activities at a site.

Special categories of unclassified information under the security cognizance of NN

UCNI, NNPI, EXPORT/IMPORT and OUO as it relates to National Security Interests of the Department/Government to include information on Critical Infrastructure that could increase the risk to our critical resources.

System

An Information System or network.

Threat

The potential that an attacker will attack a system .

NOTE: Threat is a function of the attackers' means (capability to mount a given attack) and motivation (willingness to devote resources to that attack).

User

DRAFT 11/1/96

An individual who can receive information from, input information to, or modify information on, a system without a independent human review. In a processing context, this also includes a process acting on behalf of a user. NOTE: It is often convenient to refer to a user who is NOT a privileged user as a General User.

Direct User

A user who has physical or electronic access to any component of the system.

Indirect User

A user who has access to information from the system without an independent human review, but who does not have physical or electronic access to the system, itself.

DRAFT

Privileged User

A user who has access to system control, monitoring, or administration functions (e.g., system administrator, system security officer, maintainers, system programmers, etc.).

Vulnerability

A weakness or flaw in a system; often expressed as the probability that a given attack or incident will succeed, given that the attack or incident occurs.

Net Vulnerability

11/1/96

The remaining vulnerability to a given attack, after the application of countermeasures (if any) to mitigate the system's original vulnerability.